cisco SECURE

利用 Cisco XDR 简化安全运营

增强检测成效，加快应对速度，提高工作效率

Cisco XDR 的问世，令安全团队看待检测和响应的方式为之一变。我们基于云的解决方案旨在简化安全运营，并赋能安全团队检测最复杂的威胁、确定其优先级并做出响应。Cisco XDR 与广泛的思科安全产品组合和一系列重要的第三方产品集成，是当前市场上最全面、最灵活的解决方案之一。

Cisco XDR 出自安全专家之手，专为安全业内人士打造，可以帮助分析师在一个统一的视图中汇聚并关联来自多个来源的数据，从而简化调查、减少误报、确定警报优先级，并通过最短路径快速完成从检测到响应的整个流程。

内置的自动化和协调功能以及有关补救措施的指导建议可以帮助分析师自动执行重复性任务并更有效地缓解威胁，从而腾出时间和资源，集中精力处理其他重要安全任务。

使用数据驱动的 Cisco XDR 方法，SOC 团队可以确定影响最大的事件，并将补救策略优先侧重于这些事件，从而加强组织的整体安全状况并提高弹性。

© 2023 思科和/或其附属公司。版权所有。

优势

不局限于特定供应商或攻击媒介，通过统一可视性来避免盲点

跨网络、云、终端、邮件和应用获取可视性并识别威胁，在多供应商、多媒介环境中提供有效的安全防护。

通过在一个统一的视图中关联来自多种不同检测技术的数据，Cisco XDR 能够加快和简化调查并优化事件响应。

加速威胁检测和响应，以便对真正重要的威胁采取措施

关联多个遥测源的检测结果，优先处理风险最大的威胁。

Cisco XDR 利用人工智能和机器学习技术，可以提供精准、关联的检测，减少混乱，并将安全风险与业务风险有效结合。

根据有证据支持的建议自动做出响应，最大限度地降低影响

使用自动化功能和有关威胁响应的指导建议，信心十足地在所有相关控制点消除威胁。

Cisco XDR 可以缩短调查时间并加快响应速度，无需高级别 SOC 团队也可拥有复原能力。

© 2023 思科和/或其附属公司。版权所有。

利用由数据支持的洞察，提供全面的威胁检测和响应操作

更快检测出复杂威胁

- Cisco XDR 集成了包括终端、邮件、网络、云、防火墙等的广泛设备，同时还提供部分第三方集成功能，因此 XDR 策略的灵活性、可扩展性和有效性均已登峰造极。
- 利用来自本地网络以及公共云和私有云的遥测数据，检测受管和非受管设备上的威胁并在关联事件时获取关键情景信息，包括攻击源于何处及其如何在网络中传播。
- Talos 威胁情报可增强检测能力，让分析师获得一系列无与伦比、切实可行的信息，借助更深入的情景信息和对真实威胁行为的认识来揭示已知和新出现的威胁。

按影响确定威胁的优先级，并更快地对最重要的威胁采取措施

- 根据风险确定优先级可以帮助 SOC 分析师集中精力应对构成最大威胁的警报，以便采取快速有效的操作。这种独特的方法提供了一个统一的警报视图，按实际严重性确定优先级。
- 针对威胁识别、遏制、根除和恢复提供的威胁响应指导建议与嵌入式响应操作相结合，可以实现一致且有效的决策，从而缩短平均响应时间 (MTTR)。

缩短响应时间

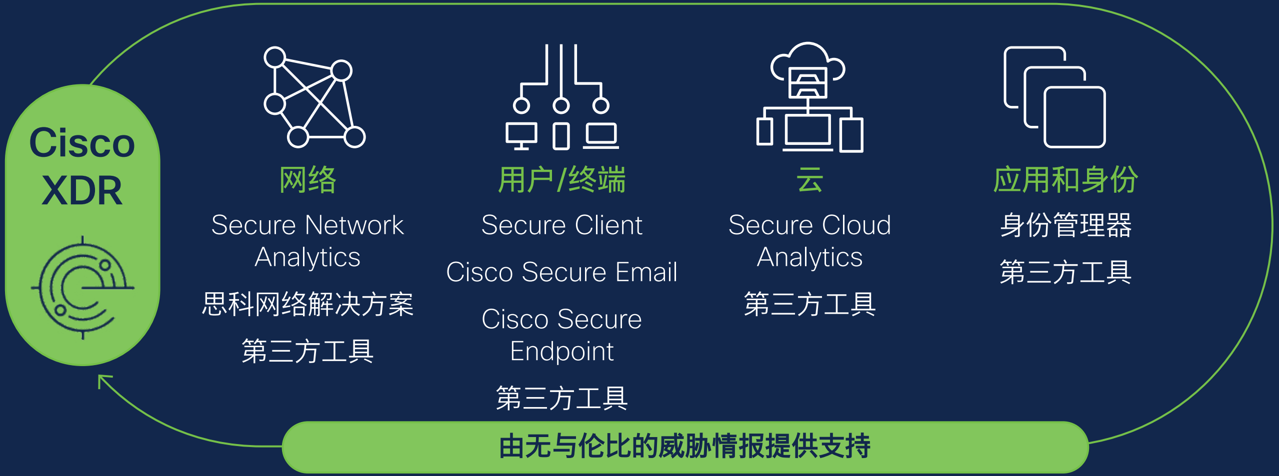
- 通过内置的响应操作和协调，迅速实施威胁补救。有了 Cisco XDR，SOC 团队就可以利用一系列预构建或可自定义的协调工作手册，只需点击几下即可帮助遏制威胁和降低风险。
- 通过自动执行耗时的重复性任务并为 SOC 团队提供现成可用的最佳实践，让有限的资源发挥出最大的价值。在不适合执行自动操作的情况下，Cisco XDR 可以提供有关威胁响应的指导建议，帮助 SOC 分析师采取有效的响应操作。
- 通过与思科解决方案和第三方解决方案中内置的各种安全控制点的深度集成，跨各种安全工具快速推送响应操作。当您获悉新的攻击策略、手法和感染指标时，您可以通过调查不同的警报日志，主动地搜寻威胁。

© 2023 思科和/或其附属公司。版权所有。

简化调查:

- 借助统一的情景信息和渐进式披露技术，简化调查并缩短调查时间。Cisco XDR 会向分析师显示完成当前任务所需的信息，不会让他们被无关数据淹没而导致分析停顿。等到需要的时候，只需点击一下鼠标即可获得更多信息来丰富调查数据。
- SOC 分析师可以汇聚警报、全球情报和本地情景信息来了解根本原因和完整影响范围，时刻准备好采取相应操作。

实施 XDR，为您提供无处不在的保护



充分利用 Cisco Security Cloud：汇集各项核心功能，包括顺畅无碍的体验、开放且可扩展的生态系统以及自动化功能

如需了解有关 Cisco XDR 的更多信息，请访问：
cisco.com/go/xdr

© 2023 思科和/或其附属公司。版权所有。Cisco 和 Cisco 徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问以下网址：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。1033963807 04/10